ESTADO LIBRE ASOCIADO DE PUERTO RICO

cdcoop

COMISIÓN DE DESARROLLO COOPERATIVO

PLAN DE CONTINUIDAD

DE OPERACIONES Y MANEJO DE DESASTRE

18 de julio de 2016

PLAN DE CONTINUIDAD DE OPERACIONES Y MANEJO DE DESASTRE

I. BASE LEGAL

Este Plan de continuidad de las operaciones y manejo de desastres de la CDCOOP, se promulga de conformidad con las facultades y poderes que le confiere la ley que crea la Comisión de Desarrollo Cooperativo de Puerto Rico (CDCOOP), Ley Número 247 de 10 de agosto de 2008, en cumplimiento a las siguientes disposiciones: Ley Número 151 de 22 de junio de 2004, según enmendada, conocida como Ley de Gobierno Electrónico, la Política Núm. TIG-015 de 30 de septiembre de 2011, según revisada, sobre el Programa de Continuidad Gubernamental, y la Política Núm. TIG-003 de 15 de diciembre de 2004, según revisada.

II. INTRODUCCIÓN

La CDCOOP reconoce que existen amenazas significativas ante la posibilidad de la ocurrencia de un incidente o desastre que afecte la operación de la agencia, como también la necesidad de recuperarse en el menor tiempo posible, garantizando la continuidad de las operaciones y los servicios. El Plan de Continuidad de las Operaciones se implementa para responder organizadamente a eventos que interrumpen la operación normal.

III. PROPÓSITO DEL PLAN

El propósito de este plan es asegurar que la CDCOOP esté preparada para responder a una emergencia, recuperarse de ella y mitigar los impactos ocasionados, permitiendo la continuidad de los servicios y funciones críticas de la agencia para la atención de las operaciones. El Plan de Continuidad de la Operaciones atiende la emergencia, administra la crisis, crea planes de contingencia y la capacidad de retorno a la operación normal.

Por medio de este plan, se establecen las normas para garantizar la continuidad operacional de las funciones críticas que la agencia maneja. Entre los objetivos del plan, se encuentra lograr un nivel de preparación necesaria frente a incidentes o emergencias que permita asegurar y proteger la integridad de los bienes de la agencia. El plan persigue establecer con antelación la planificación para minimizar pérdidas y preservar la continuidad de las funciones críticas, a través de la información esencial para poder brindar a los equipos de Sistemas de Información y propiedad de la agencia, la mayor protección ante la eventualidad de una emergencia o desastre que interrumpa las operaciones.

IV. LEYES Y REGLAMENTOS

Las políticas y procedimientos de seguridad, así como el plan de continuidad, están y deberán estar, de surgir cambios, de acuerdo a la legislación, reglamentos, cartas circulares y políticas vigentes.

V. CONTROLES FÍSICOS

El acceso a las facilidades de sistemas de información deberá estar controlados para que solamente el personal autorizado pueda utilizarlas.

Cualquier equipo usado fuera de la agencia deberá estar autorizado por la gerencia y deberá haber un procedimiento para controlar su utilización, establecido por el Comisionado.

Las facilidades de sistemas de información deberán estar colocadas en un área donde sea menor la probabilidad de daños por fuego, inundaciones, explosiones, disturbios civiles y otras formas de desastres.

VI. CONTROLES GENERALES

La CDCOOP instalará controles automáticos para la prevención y detección de programas no deseados (virus, spyware, adware y updates automáticos) provistos por la Oficina de Gerencia y Presupuesto. La seguridad de la información es parte integral del diseño de todo programa que adquiera o desarrolle la agencia para las operaciones de la CDCOOP y el servicio al ciudadano. La CDCOOP tendrá los controles necesarios para evitar, que de forma intencionada o accidental se inicien ataques desde sus redes internas hacia otros sistemas de información externos.

Los usuarios de los sistemas de información (los empleados) son responsables de mantener una copia de la información que se encuentra en el disco duro de la computadora asignada, al igual que en el "Archivo Compartido" que le será asignado, el cual almacenará la información en el servidor del centro de cómputos de la CDCOOP.

VII. PROGRMA DE PRUEBAS Y EJERCICIOS

La CDCOOP realizará al menos un ejercicio y una prueba anualmente para todas las unidades, simulando escenarios de desastres o interrupción de las operaciones de la agencia, para garantizar que el Plan de Continuidad de las Operaciones puede ser implementado en situaciones reales de emergencia y desastres. Los ejercicios y pruebas de continuidad deberán ser documentados en los siguientes formularios: "Ejercicio de Replicación de Emergencia" y en el "Formulario de Evaluación del Programa de Ejercicios y Pruebas".

VIII. EMERGENCIA DURANTE JORNADA REGULAR DE TRABAJO

De ocurrir una emergencia o desastre que afecte la agencia, los Oficiales de Sistemas de Información, notificarán sobre ello y de sus consecuencias, en primer lugar al Comisionado/a de la CDCOOP y luego al Subcomisionado/a.

IX. EMERGENCIA FUERA DE LA JORNADA REGULAR DE TRABAJO

De ocurrir cualquier emergencia durante días no laborables, los Oficiales de Sistema de Información, deberán notificar al Comisionado y al Subcomisionado/a para establecer los pasos a seguir en el Plan de Emergencia.

X. ELEMENTOS Y COMPONETES BÁSICOS NECESARIOS PARA LOS SISTEMAS DE INFORMACIÓN EN LA AGENCIA

La CDCOOP cuenta con servidores físicos y servidores virtuales. Todos los servidores físicos, así como los equipos de sistemas de información localizados en el Cuarto de Servidores, tienen que contar con el apoyo de varias baterías de respaldo para emergencias. Las baterías de respaldo deben proveer no menos de 15 minutos de carga eléctrica ininterrumpida, para permitir que se pueda almacenar, rescatar o salvar la información que se esté trabajando. De igual forma, las computadoras utilizadas por los empleados, deberán estar conectadas a una batería de respaldo para las emergencias, como fuente de energía que permita guardar o rescatar la información trabajada en casos de emergencias.

Los Servidores disponibles son los siguientes:

Servidores Físicos:

Nombre de servidor	Funciones del servidor
HV-CDCOOP-1	Servidores anfitriones "host" de servidores virtuales.
HV-CDCOOP-2	
HV-CDCOOP-3	
CDCOOP-ADMIN	Contiene aplicaciones esenciales de la agencia.
MICROMAS-H	Cuadro telefónico de la agencia
WEB-CDCOOP	Bases de datos de la agencia.

Servidores Virtuales:

Nombre del Servidor	Ubicación del Virtual	Funciones del servidor
DC-CDCOOP-1	HV-CDCOOP-3	1. **Active Directory:** contiene el directorio activo de la agencia. 2. **Domain Controller:** Mantiene el dominio de cdcoop.local. 3. **DNS:** Mantiene la comunicación por nombre dentro de la internet 4. **DHCP:** Mantiene y administra las direcciones de IP en la red interna.

SCCM-CDCOOP-1	HV-CDCOOP-3	**System Center:** Administración de centro de datos unificada.
CDCOOP-FILE	HV-CDCOOP-2	**File Server:** almacén de documentos de la agencia.
DC-CDCOOP2	HV-CDCOOP-1	**Domain Controller 2:** Mantiene el dominio de cdcoop.local
SMTP-CDCOOP-1	HV-CDCOOP-1	**SMTP Server:** Transferencia de correos electrónicos.

La Oficina de Sistemas de Información tiene que efectuar los resguardos de la información en los servidores no menos de una vez al mes.

XI. PLAN DE RESGUARDO PARA LOS SISTEMAS DE INFORMACIÓN

A. OFICINA DE SISTEMAS DE INFORMACIÓN Y USUARIOS DE ESTACIONES DE TRABAJO

Los oficiales de Sistemas de Información prepararán los resguardos de los servidores una vez al mes. Los resguardos se guardarán en la caja de seguridad ubicada en la Oficina Regional de Caguas. Cada Director Regional, es responsable de asegurarse que semanalmente todo empleado, guarde su información en el "Archivo Compartido del Servidor". Todos los resguardos estarán tanto en Caguas como en el "Centro de Cómputos" ubicado en la Oficina Central.

Es responsabilidad del empleado, tener y mantener copias de sus trabajos y archivos en el servidor, además de tenerlo en el disco duro de la estación de trabajo. La información que no se pueda recobrar del Disco Duro de la máquina, se repondrá del servidor. Es responsabilidad del empleado reproducir la información que no se encuentre en el servidor.

XII. DESATRES POR CATEGORÍAS

A. DESASTRES EN PROGRAMACIÓN

Son aquellos conflictos internos de configuración en la programación de los sistemas de información que pueden paralizar las operaciones por más de veinticuatro (24) horas.

B. DESASTRES POR ROTURAS O POR DESPERFECTOS EN PIEZAS

Las roturas o desperfectos pueden producirse en cualquier momento, sin previo aviso y sin mostrar síntomas o por razones desconocidas. Estos desastres serán reparados según la disponibilidad de las piezas de repuesto.

C. DESASTRES MENORES

Se refiere a aquellos eventos no programados o previsibles, que imposibiliten operar los equipos de Sistemas de Información, causando un impacto mínimos en el trabajo por un término no menor de una (1) hora ni mayor a veinticuatro (24) horas. Este tipo de eventos, permite que en corto tiempo se pueda comprobar la existencia de cualquier componente con desperfectos. En casos de fallas en el servicio de energía eléctrica, la determinación de equipos con desperfectos dependerá del restablecimiento del mismo. Los Sistemas de Información se repondrán con el resguardo reciente al desastre.

D. DESASTRES NATURALES

1. HURACANES, TORMENTAS E INUNDACIONES

Si en el desarrollo de cualquiera de estos fenómenos atmosféricos el empleado se encuentra en el área de trabajo deberá[1]:

1. Cerrar todos los archivos después de guardar todos los documentos en su computadora y en el servidor.
2. Apagar todos los sistemas eléctricos: monitores, baterías, bocinas impresoras, etc.
3. Desconectar los equipos de las tomas eléctricas (computadoras, impresoras y fotocopiadoras).
4. Desconectar la línea de la Red de Informática (computadoras, impresoras y fotocopiadoras).
5. Cubrir todos los equipos con sus respectivos forros plásticos o algún material que proteja el equipo (ej. Bolsas plásticas).
6. Verificar que los componentes del equipo electrónico no estén cerca de las ventanas.
7. Remover todo equipo electrónico ubicado cerca a las ventanas.

a. DURANTE EL EVENTO

Los equipos estarán guardados y protegidos en las respectivas oficinas, las cuales permanecerán cerradas.

[1] Favor hacer referencia al Memorando sobre Medidas de Seguridad durante Temporada de Huracanes, firmado por el Comisionado el día 3 de agosto de 2015.

b. DESPUÉS DEL EVENTO

Cuando el empleado regrese al área de trabajo, luego de finalizar la eventualidad, realizará una inspección del equipo. Antes de proceder a conectar el equipo en la toma de corriente, el empleado debe asegurarse que:

1. Las cubiertas no tengan agua acumulada o estén mojadas.
2. Las cubiertas no estén mal colocadas o destruidas y el equipo no esté visiblemente mojado o húmedo.
3. El monitor no esté mojado o roto.
4. La impresora no esté húmeda o mojada.
5. Los componentes no estén rotos o mojados.

De encontrar algún problema como los antes mencionados, el empleado custodio del equipo debe preparar un informe de daños el cual debe contar con lo siguiente:

1. Nombre del empleado, fecha, hora del informe.
2. Oficina en que labora y descripción la computadora, impresora y fotocopiadora.
3. Equipo considerado dañado.
4. Breve explicación de los daños.

El empleado entregará a su supervisor inmediato el informe preparado. El supervisor inmediato del empleado corroborará la información, hará constar su firma en el informe y lo enviará a la Oficina de Sistemas de Información a la mayor brevedad posible.

2. ACTIVIDAD SÍSMICA (TERREMOTO, TEMBLORES O REMESONES)

a. DURANTE EL SISMO

Los empleados no deben tener contacto directo con los equipos electrónicos.

b. DESPUÉS DEL SISMO

De encontrar algún equipo averiado, el empleado tiene que preparar un informe de daños inmediatamente y entregar el mismo a su supervisor inmediato. El supervisor inmediato del empleado corroborará la información, hará constar su firma en el informe y lo enviará a la Oficina de Sistemas de Información a la mayor brevedad posible.

De ocurrir el sismo fuera de la jornada de trabajo, el empleado debe preparar un informe de daños al regresar a sus labores.

3. FUEGO

Todo empleado deberá saber dónde están localizados los extintores de fuego.

a. DURANTE LA ALARMA DE INCENDIO

El empleado deberá:

1. Salvar o guardar en su computadora los documentos que se encuentre utilizando.

***IMPORTANTE:** El empleado debe realizar esta tarea siempre y cuando no ponga en peligro su salud o su vida.

b. DESPUÉS DEL INCENDIO

El empleado debe:

1. Entrar cuando se le autorice.
2. Revisar si hay algún equipo averiado.
3. Preparar un informe de daños de equipo inmediatamente.
4. No operar el equipo y esperar por autorización y/o asistencia.

XIII. PROCESO DE COORDINACIÓN CON OTRAS AUTORIDADES PÚBLICAS

La CDCOOP mantendrá documentado todas las actividades y procedimientos de coordinación con las diferentes autoridades públicas ante la eventualidad de un incidente y/o desastre.

XIV. ACTUALIZACIÓN DEL PLAN Y MANEJO DE CAMBIOS

La Oficina del Comisionado en conjunto con la Oficina de Informática, son responsables de la actualización del Plan de Continuidad de Operaciones, de conformidad a las leyes, reglamentos, cartas circulares y políticas aplicables.

XV. VIGENCIA DEL PLAN

El Plan de Continuidad de las Operaciones de la CDCOOP tiene vigencia inmediata luego de la firma del Comisionado de la Comisión de Desarrollo Cooperativo de Puerto Rico. Este Plan de Continuidad deja sin efecto legal cualquiera otro Plan, orden administrativa, carta circular o memorando aprobado con anterioridad.

En San Juan, Puerto Rico, hoy 18 de julio de 2016.

Hon. Sergio Ortiz Quiñones
Comisionado

EJERCICIO DE REPLICACIÓN DE EMERGENCIA
PLAN DE CONTINUIDAD DE OPERACIONES
FECHA: _____

	Actividad	Responsable	Tiempo Esperado de Duración	Hora de Inicio/Terminación (Replicación)		Cumplió	Comentarios
1.						☐ Si ☐ No	
2.						☐ Si ☐ No	
3.						☐ Si ☐ No	
4.						☐ Si ☐ No	
5.						☐ Si ☐ No	
6.						☐ Si ☐ No	
7.						☐ Si ☐ No	

Observador: _____

Oficina de Informática: _____

P.O. BOX 21408
SAN JUAN, PUERTO RICO 00928-1408
Tel. (787) 736-2097 Fax. (787) 754-3262

FORMULARIO DE EVALUACIÓN
DEL PROGRAMA DE EJERCICIOS Y PRUEBAS
PLAN DE CONTINUIDAD DE OPERACIONES

Nombre del Ejercicio/Prueba:	División o Región:	Fecha:
Nombre del Participante y Puesto:		

1. ¿Al momento del Ejercicio/Prueba, el participante tenía disponible toda la información y recursos necesarios para cumplir con sus responsabilidades?
   Ejemplo: computadoras, baterías de respaldo, "archivo compartido en servidor", documentos guardado o archivados en computadora, disco externo, "pendrive" u otros.

2. ¿Se cumplieron los objetivos del Ejercicio/Prueba?

3. ¿Qué objetivos no se cumplieron?

4. ¿Se siente preparado para efectuar sus responsabilidades de continuidad en un evento de Emergencia/Desastre? Seleccione:

No preparado _____ (Explique)	Parcialmente preparado _____ (Explique)	Preparado _____

5. Clasifique el Ejercicio/Prueba en General:

Necesita mejorar _____	Adecuado _____	Bueno _____	Excelente _____

6. Comentarios Generales:

Firma del Participante:	Fecha:
Firma del Oficial de Informática o Coordinador de Continuidad:	Fecha:

ESTADO LIBRE ASOCIADO DE
PUERTO RICO
Comisión de Desarrollo Cooperativo

Hon. Alejandro García Padilla,
Gobernador

Sergio Ortiz Quiñones,
Comisionado

3 de agosto de 2015

A TODO EL PERSONAL

Sergio Ortiz Quiñones
Comisionado

AVISO IMPORTANTE SOBRE SEGURIDAD DURANTE LA TEMPORADA DE HURACANES

La temporada de huracanes en Puerto Rico comenzó el día 1 de junio de 2015. Por tal motivo, es necesario que todos los viernes en la tarde se lleven a cabo las siguientes medidas de seguridad en cada área de trabajo:

- Organizar y proteger los equipos y materiales que estén sobre los escritorios.
- Recoger los artículos personales, si alguno, que estén ubicados en los escritorios cercanos a las ventanas, para evitar que se conviertan en proyectiles.
- Apagar los equipos electrónicos.
- Apagar la batería, que está conectada a la computadora, antes de dejar el área de trabajo.
- Utilizar bolsas plásticas para cubrir las computadoras, teclados, teléfonos, baterías y cualquier otro equipo.
- Remover todo documento de los escritorios.
- Almacenar documentos en áreas seguras, como gavetas o archivos.

Cada empleado es responsable del fiel cumplimiento de estas medidas de seguridad. En aquellos casos que el empleado esté fuera de la agencia, será responsabilidad del Director(a) Regional y/o Director(a) de Área o División, cumplir con las medidas señaladas.

Con el propósito de notificar a los empleados en caso de emergencia, los Directores(a) Regionales y/o Director(a) de Área o División, deberán mantener una lista de correos electrónicos o números telefónicos de sus empleados. La información suministrada es confidencial y para uso exclusivo en caso de emergencia.

Agradezco el fiel cumplimiento a esta directriz.

P.O. Box 21408
San Juan, Puerto Rico 00928-1408